

EXECUTIVE SECRETARIAT

ROUTING SLIP

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI		X	10/29	WIS
2	DDCI		X		
3	EXDIR				
4	D/ICS		X		
5	DDI				
6	DDA		X		
7	DDO				
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt.				
13	D/OCA	X			
14	D/PAO				
15	D/PERS				
16	D/Ex Staff				
17	D/OS/DA		X		
18					
19					
20					
21					
22					
SUSPENSE		Date			

Remarks

D/OCA to respond over his signature.



ER 88-3957X

Executive Secretary

Date

Declassified and Approved For Release 2013/12/05 :

CIA-RDP90G01353R001400130028-7

From: John L. Helgerson

17 OCT 1990

~~_____ We plan to prepare an
answer for your signature.~~

✓ We plan to prepare an answer for my signature.

No answer expected or required

John, I prefer to _____

Declassified and Approved For Release 2013/12/05 : _____

CIA-RDP90G01353R001400130028-7

EXECUTIVE SECRETARIAT

ROUTING SLIP

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI		X		
3 2	DDCI		X		
3	EXDIR				
4	D/ICS		X		
5	DDI				
6	DDA		X		
7	DDO		X		
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/OCA	X			
14	D/PAO				
15	D/PERS				
16	D/Ex Staff				
17	D/OS/DA		X		
18					
19					
20					
21					
22					
SUSPENSE		Date			

Remarks

D/OCA to respond over his signature.



ER 88-3957X

Executive Secretary

Date

2627 (10-81)

Declassified and Approved For Release 2013/12/05 :
CIA-RDP90G01353R001400130028-7

From: John L. Helgeson

17 OCT 1991

 We plan to prepare an
answer for your signature.

✓
 We plan to prepare an
answer for my signature.

 No answer expected or required


 John, I prefer to

Declassified and Approved For Release 2013/12/05 :
CIA-RDP90G01353R001400130028-7

EXECUTIVE SECRETARIAT

ROUTING SLIP

TO:

		ACTION	INFO	DATE	INITIAL
1	DCI		X		
2	DDCI		X		
3	EXDIR				
4	D/ICS		X		
5	DDI				
6	DDA		X		
7	DDO		X		
8	DDS&T				
9	Chm/NIC				
10	GC				
11	IG				
12	Compt				
13	D/OCA	X			
14	D/PAO				
15	D/PERS				
16	D/Ex Staff				
17	D/OS/DA		X		
18					
19					
20					
21			X		
22					
		SUSPENSE _____ Date			

Remarks

D/OCA to respond over his signature.

ER 88-3957X


Executive Secretary

Date

SAM NUNN, GEORGIA, CHAIRMAN

JOHN C. STENNIS, MISSISSIPPI
J. JAMES EXON, NEBRASKA
CARL LEVIN, MICHIGAN
EDWARD M. KENNEDY, MASSACHUSETTS
JEFF BINGAMAN, NEW MEXICO
ALAN J. DIXON, ILLINOIS
JOHN GLENN, OHIO
ALBERT GORE, JR., TENNESSEE
TIMOTHY E. WIRTH, COLORADO
RICHARD C. SHELBY, ALABAMA

JOHN W. WARNER, VIRGINIA
STROM THURMOND, SOUTH CAROLINA
GORDON J. HUMPHREY, NEW HAMPSHIRE
WILLIAM S. COHEN, MAINE
DAN QUAYLE, INDIANA
PETE WILSON, CALIFORNIA
PHIL GRAMM, TEXAS
STEVEN D. SYMMS, IDAHO
JOHN MCCAIN, ARIZONA

ARNOLD L. PUNARO, STAFF DIRECTOR
CARL M. SMITH, STAFF DIRECTOR FOR THE MINORITY

Received: 14 Oct 88

United States Senate

COMMITTEE ON ARMED SERVICES

WASHINGTON, DC 20510-6050

September 19, 1988

Honorable William H. Webster
Director
Central Intelligence Agency
Washington, D.C. 20505

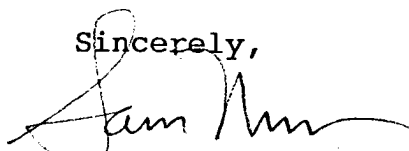
Dear Mr. Webster:

In December of 1987 the Committee on Armed Services implemented a formal set of security procedures to strengthen and enhance our handling and protection of national security information. A copy of these procedures is enclosed. These procedures have been brought to your attention previously, but I want to reemphasize them and particularly direct your attention to Sections VII and VIII on page 6 which deal with Executive Branch departments and agencies and the receipt of classified information in Committee.

To be successful, these procedures will depend in no small measure on the cooperation we are able to receive from members of your agency. For your information, the Committee's Security Control Officer is Ms. L. Monica Chavez and she may be reached on 224-5298 should members of your office have any questions.

I hope that you will instruct all appropriate personnel in your agency of the Committee's requirements with respect to classified materials. Your cooperation will be very much appreciated.

Sincerely,



Sam Nunn
Chairman

Enclosure

L-231-1r

SAM NUNN, GEORGIA, CHAIRMAN

JOHN C. STENNIS, MISSISSIPPI
J. JAMES EXON, NEBRASKA
CARL LEVIN, MICHIGAN
EDWARD M. KENNEDY, MASSACHUSETTS
JEFF BINGAMAN, NEW MEXICO
ALAN J. DIXON, ILLINOIS
JOHN GLENN, OHIO
ALBERT GORE, JR., TENNESSEE
TIMOTHY E. WIRTH, COLORADO
RICHARD C. SHELBY, ALABAMA

JOHN W. WARNER, VIRGINIA
STROM THURMOND, SOUTH CAROLINA
GORDON J. HUMPHREY, NEW HAMPSHIRE
WILLIAM S. COHEN, MAINE
DAN QUAYLE, INDIANA
PETE WILSON, CALIFORNIA
PHIL GRAMM, TEXAS
STEVEN D. SYMMS, IDAHO
JOHN MCCAIN, ARIZONA

ARNOLD L. PUNARO, STAFF DIRECTOR
CARL M. SMITH, STAFF DIRECTOR FOR THE MINORITY

United States Senate

COMMITTEE ON ARMED SERVICES
WASHINGTON, DC 20510-6050

December 18, 1987

MEMORANDUM

TO: Staff of the Committee on Armed Services and S. Res. Designees

FROM: Senators Nunn and Warner

SUBJECT: Security procedures

We have promulgated a formal set of security procedures, a copy of which is attached. Although these procedures embody the past practices of our Committee, there are important new safeguards with which you must become familiar.

Our staff has demonstrated that it is capable of protecting classified information. However, we must never become complacent about the protection of classified information. Because our committee is responsible for classified information pertaining to national defense, it is imperative that strict adherence to these procedures be maintained at all times. To ensure that all members of the staff receive and read these procedures, an acknowledgement block is at the bottom of this form.

TO: Chief Clerk, SASC

I have received and read "Senate Armed Services Security Procedures," dated December 18, 1987. I agree to adhere to the procedures set forth in that document, and understand that failure to do so may result in disciplinary action against me, up to and including dismissal.

(typed name)

(date)

(signature)

DECEMBER 18, 1937

SENATE ARMED SERVICES SECURITY PROCEDURES

I. GENERAL

A. This document establishes security procedures applicable to the Senate Armed Services Committee (SASC) staff and personal staff of Committee Members designated to the SASC by that Member under Senate Resolution 4, 95th Congress. It also covers any personnel who are granted access to classified information or proceedings under the control of the Committee. It covers (1) security clearances; (2) access to classified information; (3) disclosure of classified information; (4) control and storage of classified documents; (5) removal of classified information from Committee spaces; (6) the notice to Departments and Agencies of these procedures; (7) the receipt of classified material in Committee spaces; (8) the logging in procedures, operating standards, reproduction and destruction of classified materials; (9) the training of personnel on security procedures; (10) security checks; and (11) the conduct of classified hearings.

B. Senate Resolution 4, 95th Congress, (portions of which are codified at 2 U.S.C., 72a-1e) provides that a Senator may designate "employees in his office to assist him in connection with his membership on committees of the Senate. . . . Such employees shall be accorded all privileges of a professional staff member . . . except that any such committee . . . may require, if classified material is being handled or discussed, that any staff member possess the appropriate security clearance before being allowed access to such material or to discussion of it." For purposes of this document, employees of Senators designated to the Senate Armed Services Committee are hereinafter referred to as "S. Res. designees."

C. Unauthorized disclosure of classified information is a crime (e.g., 18 U.S.C. 792-99, 952; 50 U.S.C. 421-26, 783). Committee staff and S. Res. designees must exercise great care in handling, storage, and dissemination of classified information.

D. For purposes of this document, the term "classified information" means any document, information, or material, regardless of its physical form or characteristics, that has been classified by the Executive Branch or the Congress as requiring protection against unauthorized disclosure in the interests of national security.

E. Committee offices shall operate under strict security precautions. All classified information shall be handled in strict accordance with the procedures in this document except to the extent that separate, more stringent procedures are provided for daily intelligence packages. Staff members who fail to follow these procedures or other applicable rules or statutes governing classified information are subject to disciplinary action, including dismissal. If warranted, violations of security procedures may be referred to the Attorney General for possible criminal proceedings.

II. SECURITY CLEARANCES

A. To facilitate security procedures, the Committee recognizes security clearances granted by authorized Executive Branch agencies.

B. When these procedures require a new clearance or an updated clearance, the investigation will be performed by the FBI, and the clearance adjudication will be made by the Department of Defense. The Department of Defense may, as they deem appropriate, conduct an independent investigation. CIA shall adjudicate the granting of clearances for Special Compartmented Information (SCI, commonly referred to as "codeword".) SCI access, under CIA regulations, shall be granted only to members of the Committee staff and strictly on a need-to-know basis.

1. A current or prospective Committee staff member or S. Res. designee who does not hold a current Top Secret clearance shall complete the forms necessary for an FBI background investigation. The Chairman (or the sponsoring Member, in the case of an S. Res. designee) will request the FBI to conduct the background investigation required for a Top Secret clearance.

2. The clearances of Committee staff members and S. Res. designees must be current, including a periodic reinvestigation by the FBI every five years. The Chairman (or the sponsoring Member in the case of an S. Res. designee) shall request the FBI to update the investigation of any staff employee whose clearance has not been granted or updated within 5 years.

3. In the case of a current or prospective member of the Committee staff, the results of the FBI investigation or reinvestigation will be forwarded to the Department of Defense for an adjudication of the clearance request.

C. In the case of an individual who also requires access to information under the control of the Department of Energy (e.g., a "Q" clearance), the Chairman or the sponsoring member, shall request the Department of Energy to conduct the appropriate investigation and adjudicate the granting of the clearance.

D. In the case of a current or prospective Committee employee or S. Res. designee, the Chairman (or the sponsoring Member, in the case of an S. Res. designee) shall request the agency that granted the clearance to forward the results of the investigation or reinvestigation and the appropriate documentation to the Chairman or the sponsoring Member, as appropriate. The Staff Director shall insure that all material relating to minority Committee staff members is available to the Ranking Minority Member and Minority Staff Director.

III. ACCESS TO CLASSIFIED INFORMATION

A. Access to classified information under the control of the Committee is governed by these procedures and shall be granted only to those having a need-to-know. No one has a right to such access solely by virtue of rank, position, or security clearance.

B. Unless otherwise directed by the Chairman, access to classified information under the control of the Committee shall take place in the Committee's offices and is restricted to:

1. Members of the Committee
2. Senators who are not members of the Committee by permission of the Chairman.
3. The Staff Director and Minority Staff Director, subject to the guidance of the Chairman.
4. The following persons if possessing a valid security clearance as documented to the Chairman and when there is a valid need to know as determined by the Chairman: (1) a member of the Committee staff; (2) an S. Res. designee; or (3) a personal representative of the Majority or Minority Leader.

IV. DISCLOSURE OF CLASSIFIED INFORMATION

A. No person who has acquired classified information under the control of the Committee shall disclose, in whole or in part or by way of summary, for any purpose or in connection with any proceeding, judicial or otherwise, any classified information under the control of the Committee or any testimony given before the Committee in executive session, including the contents of any papers or other materials or other information received by the Committee, except as specifically authorized by the Committee or the Senate or as provided in Section III.B. of these procedures.

B. When preparing questions for Senators' use at hearings, care must be taken to ensure that questions for open hearings do not contain classified information. If the session is closed for national security reasons (i.e. executive session), questions containing classified information must be marked as classified. This is especially important if the question is not asked at the session but is submitted for the record.

V. CONTROL AND STORAGE OF CLASSIFIED DOCUMENTS

A. The Staff Director is responsible for the maintenance, under appropriate security procedures, of a registry which will number and identify all classified information received or generated by the Committee. Such registry shall be available for review by any Senator or staff member of the Committee. The Staff Director shall designate a Security Control Officer and such assistants as may be necessary to exercise responsibility for control of classified information.

B. All classified information received in or generated by the Committee shall be delivered to and logged in at the Committee's office in Room 228 of the Russell Senate Office Building. In addition, it is the responsibility of each staff member to insure that all classified information coming into his or her possession is entered into the log system as described in Section IX. All classified information shall be stored in safes in the Russell Senate Office Building offices for Committee use and safekeeping, except that all special compartmented information, commonly known as "codeword", and all "special access" information will be stored only in the DoD and CIA authorized and approved storage area designated for "codeword" and "special access" materials. All "codeword" and "special access" information must be stored in the approved location by the Staff Director.

C. Classified information must be stored in secure storage containers (combination lock safes) and may be examined only at locations within the office that are secure.

D. Copying or duplicating such information is prohibited except in accordance with Section XI of these procedures. All copies shall be logged in as provided for in Section IX.

VI. REMOVAL OF CLASSIFIED INFORMATION FROM COMMITTEE SPACES

A. Any permanent removal or transfer of classified information from the Committee spaces shall be noted by the Security Control Officer in the classified registry. Staff members may hand-carry classified information to meetings within the Capitol complex in direct connection with their Committee responsibilities. Such classified information is to be transported in accordance with Section VI.E.

B. Transmittal of classified information by the Security Control Officer upon authorization of the Chairman or Staff Director to a Member of the Committee shall be accomplished by the Security Control Officer to the sponsoring Member's S. Res. designee (if holding an appropriate security clearance) under receipt. Whenever the Committee makes classified information available to any other committee of the Senate or to any member of the Senate not a member of the Committee, the material shall be transmitted by the staff of this Committee under the procedures outlined in this paragraph.

C. Transportation of classified information outside the Capitol complex shall be accomplished by DoD courier or Department of State Courier System or as otherwise authorized by the Chairman or Staff Director. The Security Control Clerk shall require a receipt from the courier and the recipient of the information.

D. Classified information to be transported outside the Committee by DoD or Department of State courier, will be contained in two opaque envelopes or sealed containers. Only the inner envelope or container will contain the classification markings. The outer envelope will be free of any indications that classified material or information is enclosed.

E. As authorized by the Chairman or Staff Director, classified information may be removed from Committee spaces by the Committee staff only to the extent necessary for use by a Member. Classified material removed from the Committee for a Members' review must be in a folder with a classified cover sheet or other exterior markings clearly indicating that it contains classified information.

VII. NOTICE TO DEPARTMENTS AND AGENCIES

A. All Departments and Agencies shall be advised in writing that:

1. Unless directed otherwise by the Chairman or Staff Director, all classified information must be delivered to the Security Control Officer in Room SR-228 between the hours of 9:00 a.m. and 5:00 p.m., Monday-Friday.
2. All classified information must be addressed to the SASC Chairman, the SASC Ranking Minority Member, or a SASC staff member. The Committee will not accept classified material addressed to S. Res. designees or other personal staff of the Senate.
3. All classified information must be transmitted with a multiple copy receipt and the signature of the Security Control Officer accepting receipt must be obtained.

B. "Special Access" will be delivered only for specifically named SASC staff members who hold the required clearances. All such material shall be delivered to and signed for by the Chief Clerk unless it can only be delivered to and signed for by the Staff Director. All such material will be included in the logging procedures outlined in Section IX.

VIII. RECEIPT OF CLASSIFIED INFORMATION IN COMMITTEE

A. When presented with a classified document or other classified information by courier or by a staff member, the Security Control Officer will verify that the addressee is authorized to receive the document. If not, the Security Control Officer may not accept the document. If the addressee is authorized to receive the document, the Security Control Officer will sign the receipt and complete any other requested information. The courier should leave with the Security Control Officer at least one copy of the signed receipt attached to the document. The Security Control Officer will log the document in the classified registry and assign a control number to the document.

B. Unless otherwise directed by the Staff Director, no staff member other than the Chief Clerk, the Security Control Officer, or a person designated by the Staff Director to assist the Security Control Officer, is authorized to sign a receipt for any classified information.

IX. LOGGING PROCEDURES

A. Immediately upon receipt, the Security Control Officer will assign a control number and log in the information using the classified registry. This registry is the log for all classified information received in the Committee and will be retained by the Security Control Officer. It will contain a description of the information, the level of classification, the control number assigned to it and the date received.

B. The Security Control Officer will also indicate the name of the staff member to whom the information is being routed and where it will be stored. All classified information addressed to the Chairman will go to the Chief Clerk and all classified information addressed to the Ranking Minority Member will go directly to the Minority Staff Director or his designee for storage, filing, or destruction.

C. Once the classified information has been logged in, the Security Control Officer will prepare a classified information control card. The original of the classified information control card shall be attached to the agency transmittal receipt and kept by the Security Control Officer. A duplicate of the control card will be attached to the classified document underneath the classified document cover sheet by the Security Control Officer. The control card will remain with the document.

D. Staff members will be held fully responsible for safeguarding, controlling, and accounting for classified information received by them. Upon departure from Committee employment, staff members must account for all classified material assigned to them.

X. COMMITTEE OPERATING STANDARDS, SAFES, AND MARKING OF DOCUMENTS

A. Every staff member is responsible at all times for safeguarding classified information within our offices. In addition, however, a staff member will be assigned certain additional duties in each respective office area in which safes are located. This person is responsible for oversight of the protection of classified information in their areas. The person will monitor access to safes in their areas, and they will control access to the safes and will secure the safes in their designated areas. They will also maintain a record of the time and date when the safes were opened and closed.

B. A reversible "OPEN/CLOSED" sign will be affixed at all times to the safe. No extraneous material is to be kept on top of the safes.

C. The overall classification of a document, shall be conspicuously marked or stamped at the top and bottom on the outside of the front cover (if any), on the title page (if any), on the first page, on succeeding pages, and on the outside of the back cover (if any) with the appropriate classification level.

D. Classified information in another physical form (e.g., computer tapes or slides) shall also be conspicuously marked with the highest level of classification of the material contained therein.

XI. REPRODUCTION OF CLASSIFIED INFORMATION

A. Classified information may not be reproduced, except as authorized by the Chairman or Staff Director.

B. All such copies must be logged in as provided in Section IX.

C. All classified information generated by the Committee is to be typed only on one of the two TEMPEST computers available in the Committee offices. All disks will be stored in the Committee safes. All waste generated will also be stored in the Committee storage containers. Classified information may not be typed or stored on the Committee's Data General computer system or on free-standing typewriters.

XII. DESTRUCTION OF CLASSIFIED INFORMATION

Special waste containers will be designated for classified information. Destruction of classified information will be accomplished by the Department of Defense. A DoD courier will pick up the information to be destroyed every other Wednesday. The dates of destruction will be noted on the classified control card and in the registry. Anyone failing to notify the Security Control Officer of the destruction of a document will be held accountable for material that may have been destroyed but for which no record of destruction exists.

XII. TRAINING PERSONNEL

The Staff Director shall insure that all personnel are trained in appropriate security procedures and are familiar with the laws and regulations in this area. A record of such training shall be maintained in each staff member's personnel file.

XIV. SECURITY CHECK

The Staff Director shall insure that periodic security checks are performed in all Committee spaces. Regularly scheduled technical assessments will be conducted by appropriate personnel. Records of such reviews will be maintained by the Chief Clerk.

XV. CONDUCT OF CLASSIFIED HEARINGS

In addition to the procedures authorized in this paper, the Staff Director shall insure that the following minimum standards are followed for the conduct of classified hearings:

1. The Staff Director or his designee shall insure that only personnel holding appropriate security clearances are present.

2. The Staff Director or his designee shall insure that the clearances of Executive Branch personnel are verified by the agency representative at the hearing and that a record of all those from the Executive Branch in attendance is provided for the permanent hearing record.

3. The Staff Director shall insure that the appropriate pre-hearing and during-the-hearing measures are in place for all classified hearings and for those hearings deemed particularly sensitive.